

Patent claims

1. A method for authenticating a smart card (*SIM*) in a messaging network, preferably a GSM network, wherein an algorithm and a secret key are stored in a smart card (*SIM*), whereby for authentication
  - the network or a network component first transfers a random number (*RAND*) to the smart card,
  - a response signal (*SRES*) is generated therefrom in the smart card by means of the algorithm and the secret key ( $K_i$ ) and transmitted to the network or network component,
 characterized in that
  - to form an authentication parameter the secret key ( $K_i$ ) and the random number (*RAND*) are each split into at least two parts ( $K_1, K_2; RAND_1, RAND_2$ ),
  - one of the parts ( $RAND_1, RAND_2$ ) of the transferred random number (*RAND*) is encrypted with the aid of one or more parts ( $K_1, K_2$ ) of the secret key ( $K_i$ ) by means of a one- or multistep, preferably symmetrical algorithm, and
  - a given number of bits is selected from the encryption result and transferred as a signal response (*SRES*) to the network.
2. A method according to claim 1, characterized in that the secret key ( $K_i$ ) and/or the random number (*RAND*) are split into two parts.
3. A method according to claim 1 or 2, characterized in that a part of the transferred random number (*RAND*) and one and/or more parts of the secret key ( $K_i$ ) are used to calculate a channel coding key ( $K_c$ ) by means of a one- or multistep algorithm, at least one part of the calculation result being used as the channel coding key ( $K_c$ ).
4. A method according to any of claims 1 to 3, characterized in that the key ( $K_i$ ) and the random number (*RAND*) are split into two equally long parts ( $K_1, K_2/ RAND_1, RAND_2$ ).

5. A method according to any of claims 1 to 4, characterized in that DES algorithms are used to calculate the authentication parameters ( $SRES$ ,  $SRES^*$ ) and/or the channel coding key ( $K_c$ ).
6. A method according to any of claims 1 to 4, characterized in that the, preferably one-step, IDEA algorithm is used to calculate the authentication parameters ( $SRES$ ,  $SRES^*$ ) and/or the channel coding key ( $K_c$ ).
7. A method according to any of claims 1 to 4, characterized in that a compression algorithm whose output value has a smaller length than the input parameter is used to calculate the authentication parameters ( $SRES$ ,  $SRES^*$ ) and/or the channel coding key ( $K_c$ ).
8. A method according to any of claims 1 to 7, characterized in that the calculation is effected in an at least two-step algorithm.
9. A method according to any of claims 1 to 8, characterized in that a triple DES algorithm is used as an encryption algorithm, whereby one first encrypts with the first part ( $K_1$ ) of the key ( $K_i$ ), then decrypts with the second part ( $K_2$ ) of the key ( $K_i$ ) and thereupon encrypts again with the first part ( $K_1$ ) or a third part of the key ( $K_i$ ).
10. A method according to any of claims 1 to 9, characterized in that a selection of the first or second part of the random number ( $RAND$ ) is effected in the same way in the card and the network in random or pseudorandom alternation.